DEPARTMENT OF THE ARMY
HEADQUARTERS, 4TH INFANTRY DIVISION
FORT HOOD, TEXAS 76544

AFYB-CG 22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 11: Rules of Behavior

1. References:

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

   f. DoD Instruction 5200.4- DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

2. Purpose of Policy: Automated information systems (AIS) and communications resources provided are intended for official and approved use only. This policy describes the rules of behavior that govern using these resources.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Non-compliance: This policy is punitive. Violators may be subject to action under the UCMJ, administrative action, or other federal or state law.

5. Responsibilities:

   a. Commanders, Directors, and supervisors at all levels shall ensure that subordinate personnel are aware of their individual responsibilities to protect these valuable resources and use them in an authorized and effective manner. Unauthorized or inappropriate and careless use may be a basis for disciplinary action.

   b. The 4ID user community shall utilize automated resources responsibly and abide by normal standards of professional and personal conduct at all times.

   c. All 4ID personnel and tenants shall report suspected security risks and unauthorized activity to their respective Information Assurance Manager (IAM), Information Assurance Network Manager/Officer (IANM/O), Information Assurance Security Officer (IASO), or Systems Administrator (SA).

Manager/Officer (IANM/O), Information Assurance Security Officer (IASO), or Systems Administrator (SA).

d. All personnel assigned, attached, and/or subject to this command shall:

(1) Ensure that appropriate Rules of Behavior policies are established.

(2) Empower the IAPM to develop procedures to ensure that the Rules of Behavior are being properly administered, disseminated, and followed.

e. The 4ID IAM shall develop procedures designed to verify that Rules of Behavior are understood by all 4ID soldiers, civilians, and contractors, and that said rules are being properly administered and followed. The IAM, in addition to other duties, shall have the following responsibilities:

(1) Work with the Staff Judge Advocate (SJA) to develop a statement of acknowledgment for each user to sign as a confirmation that they understand and intend to abide by the Rules of Behavior and related policies. The IAM and JAG shall review the language in the acknowledgment for adequacy on an annual basis.

(2) Appoint an Information Assurance Security Officer (IASO) and an assistant IASO with responsibility to audit the acknowledgement statements on an annual basis; and, to provide security awareness briefings as required in support of this policy.

(3) Ensure the Rules of Behavior policy is enforced.

6. Policy: This policy provides direction for 4ID personnel and tenants as it relates to a) authorized access, b) protection of information and computer ethics, c) use of copyrighted material, and d) software code of ethics.

a. Authorized Access to Networks and Systems:

(1) The U. S. Army makes available computer networks, communication systems, and software to enable military and civilian employees, contractors, and others to work efficiently and provide high-quality, high-tech service to its customers. The Army also provides access to the Internet to facilitate communication with outside contractors, vendors, and affiliates. All personnel shall use these resources only for official business or otherwise approved purposes. Moreover, when using these resources, all personnel shall abide by the U. S. Army's policies and procedures with regard to access, protection of information and property, and observation of copyright laws.

(2) There are data security risks inherent in using the Internet. Therefore, the U.S. Army reserves the right to monitor connectivity requests, messages, and material transmitted over the Internet and government provided information and communications resources. Personnel who use the Internet and government provided communications resources in an inappropriate manner, or who violate the integrity of restricted information of the U.S. Army and affiliates, or who send messages or materials which are not consistent with the U.S. Army's policies or appropriate workplace conduct, may be subject to disciplinary action.

(3) Personnel who abuse or misuse access privileges or gain unauthorized entry into U.S. Army information systems, internal or external networks, or user files (i.e., hacking) are subject to disciplinary action. Disciplinary action may also be taken in the event of unauthorized access to another person's voice mail. In some cases, the abuse of access privileges may be illegal, and the violator may be subject to civil and criminal penalties.

b. Protection of Information and Computer Ethics

(1) Safeguards and password requirements established by 4ID policies serve to protect the confidentiality, integrity, and availability of information exchanged over official networks. When working on proprietary or sensitive information, 4ID personnel shall use passwords to prevent unauthorized access to their files and shall take appropriate actions to prevent unauthorized personnel from viewing these materials on monitors.

(2) Personnel who use the Internet need to be aware that information communicated over the Internet is accessible by the public and can easily be intercepted and accessed illegally. Therefore, Internet users shall take the following precautions to control inherent Internet risks:

(a) Refrain from discussing any sensitive information over the Internet.

(b) Never give access or passwords for U.S. Army computer systems or accounts to anyone over the Internet.

(c) Obtain authorization from the IANM/IASO before making the internal resources of U.S. Army systems (e.g., email, FTP server, etc.) available to external Internet users (e.g., vendors, affiliates, etc.).

(3) 4IDpersonnel shall not use work time or government provided Internet access to conduct activities for personal profit. Government AIS will not be used to access gambling or pornographic web sites.

(4) The following activities are prohibited:

a) Hateful, harassing, or other antisocial behavior
b) Intentional damage or interference with others (like the Internet Worm)
c) Accessing or creating obscene files
d) Release of information about the Government which has not been approved for disclosure
e) Disclosure of restricted information to unauthorized recipients
f) Sending sensitive but unclassified or strategic information in clear text (unencrypted) over the Internet
g) Hacking or attempting to hack into AIS
h) Other inappropriate activities

(5) Chain letters generate excess traffic on email networks, take disk space on our email servers, and perform no useful function. Do not respond to chain letters. Delete these messages.

c. Use of Copyright-Protected Material

(1) Most texts, photographic, and graphic material in books, magazines, external databases, and other published sources, including electronic sources, are protected by copyright. Reproducing and/or distributing copyrighted material without first obtaining the permission of, or purchasing reproduction rights from, the copyright holder is likely to be a copyright infringement. Reproduction and distribution includes electronically scanning, or otherwise copying, materials for inclusion in reports, brochures, or other documents. The U.S. Army will not tolerate copyright violations. Those who make unauthorized use of copyright protected material are subject to disciplinary action.

(2) Personnel desiring additional information copyright laws and infringement may contact the office of the Staff Judge Advocate (SJA) or United States Attorney.

d. Software Code of Ethics

(1) The U.S. Army makes software packages available to its personnel through:

(a) Site licenses - for software that may be used on assigned desktop workstations and, with authorization, on home computers (e.g., anti-virus software)

(b) Volume licensing agreements - for other packages that contain use-specific restrictions (e.g., restricted to use on notebook computers, etc.)

(c) Concurrent-use licenses - for applications that are under key control (e.g., Adobe Illustrator, etc.)

(d) Individual copy licenses - for software purchased for individual use.

(e) All software must be purchased through the Army Small Computer System. Waivers are required to purchase software outside of this venue. See: https://ascp.monmouth.army.mil

(2) The U.S. Army has a strict policy concerning software duplication to ensure that personnel comply with copyright and trademark laws around the world and use software in accordance with applicable license agreements.

(3) Any duplication of software, except for backup and archival purposes, is contrary to the policies of the U.S. Army and may be a violation of copyright or other laws. Observing the following guidelines should help personnel understand and comply with policies, applicable laws, and software license agreements:

(a) Use software in accordance with the terms of the license agreements.

(b) Purchase all software for use on Government computers through the procurement process.

(c) Do not give unauthorized copies of software to anyone (including, but not limited to, customers, family members, friends, affiliates, or vendors).

(d) Notify the IAM, IANM, or IASO of any suspected misuse of software within the NCR.

(4) The 4ID shall not tolerate the use of unauthorized copies of software. Licensed software will be provided to all personnel who require it in connection with their work. Personnel who copy, use, or otherwise acquire unauthorized software are subject to disciplinary action. In addition, personnel shall be aware that anyone illegally reproducing software may be subject to civil and criminal penalties.

(5) Personnel shall contact the IAM, IANM, or IASO with questions regarding these guidelines.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding